

Das Hochsicherheits-Windows



c't-Tool aktiviert Profi-Schutz

Erpressungstrojaner sind weiterhin schwer in Mode bei Kriminellen, denn mit ihnen lässt sich leichtes Geld verdienen, weil Windows bei Privatnutzern üblicherweise offen steht wie ein Scheunentor. Das liegt auch daran, dass Microsoft ihnen Sicherheitsfunktionen vorenthält. Ein c't-Tool ändert das.

Von Axel Vahldiek

Windows-PCs in Firmen sind oft so sehr verrammelt, dass man auf ihnen nur jene Anwendungen starten kann, die zuvor vom Administrator ausdrücklich genehmigt wurden. Das soll nicht nur verhindern, dass die Mitarbeiter spielen statt zu arbeiten, sondern schützt auch zuverlässig vor vielen Viren und Trojanern. Zwar gibt es mittlerweile jene seltenen Schädlinge, die sich dateilos ins System einnisten [1], doch die meisten arbeiten anders: Ein Skript auf einer befallenen Website oder ein Makro in einem infizierten Dokument lädt die eigentliche Schädlingsdatei auf die Festplatte herunter und trägt einen passenden Autostart ein, der dafür sorgt, dass die Programmdatei beim Hochfahren des Systems mit gestartet wird. Wenn sie aber nicht in der Liste der genehmigten Anwendungen steht, scheitert auch ihr Start und der Schädling kann nichts anrichten. Das Gleiche gilt auch für Malware, die als ausführbare Datei etwa per Mail beim Nutzer ankommt. Der Mechanismus, der dahintersteckt, heißt „Software Restriction Policies“ (SRP). Dabei handelt es sich letztlich um Listen von erlaubten sowie verbotenen Anwendungen und Dateitypen. Bei neueren Windows-Versionen gibt es eine noch etwas mächtige Variante davon namens Applocker, für den Schutz vor Krypto-Trojanern reichen die bereits mit Windows XP eingeführten SRP aber völlig aus.

Privatanwendern half das bislang allerdings nichts, denn den Home-Editionen von Windows fehlen die zum Konfigurieren der SRP nötigen Werkzeuge – und das, obwohl SRP an sich auch unter Home funktionieren. Wir lösen das Problem: Mit unserem Programm „Restric'tor“ können Sie SRP in allen Windows-Editionen gleichermaßen konfigurieren und verwalten.

Dieser Beitrag erläutert, was SRP eigentlich sind, welche Auswirkungen sie haben und wie Sie auf dem eigenen PC auch ohne Aktivieren der SRP vorab prüfen können, was nach dem Aktivieren wohl alles blockiert werden würde. Das erleichtert die Entscheidung, auf welchen Rechnern Sie SRP wirklich einsetzen wollen, denn eines muss deutlich gesagt werden: SRP sind zwar für viele, aber nicht für alle PCs geeignet. Der nachfolgende Artikel erklärt den Einsatz unseres Werkzeugs Restric'tor und gibt Handreichungen, wie Sie Windows dazu bringen, Sie von sich aus über Verstöße gegen Ihre selbst erstellten Regeln zu informieren. Es folgen Tipps, wie Sie bereits vor dem ersten Start einer Anwendung erkennen können, ob Sie womöglich einen Schädling vor sich haben.

Ein Virenscanner reicht längst nicht mehr.

Falls Sie jetzt ob der Länge der Artikelstrecke zurückschrecken: In der Tat, auch wenn wir mit unserem Restric'tor versuchen, Ihnen möglichst viel Aufwand abzunehmen, kann das Konfigurieren und Pflegen von SRP dennoch mit einem gewissen Aufwand verbunden sein – je nach Einsatzzweck einer Windows-Installation reicht die Bandbreite dabei von Einrichten und Vergessen bis hin zu ständig nötiger Pflege. Sie profitieren aber im Gegenzug von einem für Privatanwender bislang unter Windows unerreichbaren Schutz-Level. Lesen Sie sich also in Ruhe die Artikel durch und wägen Sie danach ab, wie viel Aufwand der Einsatz von SRP auf Ihren Rechnern wohl bedeutet und ob Ihnen der Sicherheitsgewinn das wert ist. Und denken Sie dabei auch an jene PCs, für die Sie im Freundes- und Familienkreis den Admin spielen: Nach unseren Erfahrungen wird Schwiegermutter von aktiven SRP üblicherweise gar nichts merken. Und wenn Sie künftig nicht mehr ständig wegen Virenbefall zu Hilfe gerufen werden, haben Sie selbst dann etwas von SRP, wenn Sie sie auf dem eigenen Rechner gar nicht nutzen.

An der UAC vorbei

Zuerst noch ein paar weitere Worte dazu, warum eine Standard-Windows-Installation auch heutzutage noch offen wie ein Scheunentor ist. Denn immerhin hat Microsoft in den letzten Jahren ja einige Anstrengungen dagegen unternommen. So ist seit dem Service Pack 2 für Windows XP eine Firewall an Bord und seit Windows 8 ein Virenscanner. Seit Vista arbeiten die Nutzer zudem üblicherweise mit eingeschränkten Benutzerrechten, und zwar selbst dann, wenn sie als Administrator angemeldet sind. Um letzteres kümmert sich die Benutzerkontensteuerung, englisch „User Account Control“ (UAC).

Die UAC sorgt dafür, dass jeder Prozess, den ein als Administrator angemeldeter Anwender startet, trotzdem erst mal nur mit eingeschränkten Rechten läuft.

C:\Users\axv\Downloads\Rechnung.doc.exe

Dieses Programm wurde vom Systemadministrator geblockt. Weitere Informationen erhalten Sie vom Systemadministrator.

OK

Software Restriction Policies (SRPs) sorgen dafür, dass nur noch zuvor genehmigte Anwendungen starten – Schädlinge werden hingegen blockiert.

Das gilt selbst für den Explorer. Mangels Admin-Rechten hat man unter anderem nicht mehr überall Schreibrechte: Sie fehlen beispielsweise im Windows- und im Programme-Ordner. Möchte ein Prozess dort etwas hinschreiben oder hinkopieren, muss er bereits mit Administratorrechten gestartet worden sein oder sie sich nachträglich verschaffen. Beides löst eine der bekannten „Sind Sie sicher?“-Nachfragen aus. Alle weiteren Prozesse starten trotzdem wieder mit eingeschränkten Rechten.

Die Nachfragen sind immer dann etwas nervig, wenn man gerade selbst geklickt hat, da man sich ja üblicherweise schon beim ersten Klick sicher war. Sollte hingegen eine Sind-Sie-sicher-Frage aus dem Nichts erscheinen, versucht wohl irgendein Programm im Hintergrund, sich Administratorrechte zu verschaffen – und es besteht immer die Gefahr, dass das ein Schädling ist. Und wenn man in so einem Moment einfach so auf „ja“ klickt, hat man verloren, falls es es sich wirklich um einen Schädling handelt. Denn ein Prozess mit Admin-Rechten darf genau alles auf dem System. Zwar kann man selbst Administratoren Rechte wegnehmen, doch wenn ein Prozess erst mal mit vollen Rechten läuft, kann er sich fehlende Zugriffsrechte einfach wieder selbst einräumen. Allenfalls der Virenscanner könnte in diesem Moment noch einschreiten, doch ein mit Admin-Rechten laufender Schädling kann sich vor dem problemlos verstecken oder ihn einfach abschalten.

Die Schädlingsprogrammierer gehörten zu den ersten, die begriffen, dass UAC-Nachfragen den Benutzer auf einen Angriff hinweisen können. Daher unterlassen ihre Machwerke längst alle Aktionen, die so eine Nachfrage auslösen könnten. Wozu auch? Wenn ein Erpressungstrojaner den UAC-geschützten Windows-Ordner verschlüsseln würde, könnte man Windows einfach neu installieren. Die ohne UAC-Abfrage verschlüsselbaren Ordner im Benutzerprofil hingegen enthalten die persönlichen Bilder, Videos und Dokumente des Benutzers, und wer davon kein Backup hat, lässt sich viel leichter zur Zahlung von Lösegeld erpressen. Weil zudem auch für Nutzer mit eingeschränkten Rechten Stellen existieren, an denen sie Autostarts eintragen können, können sich Schädlinge problemlos auch ohne Administratorrechte auf Dauer einnisten – genau deshalb ist Windows in der Standardeinstellung wie erwähnt offen wie ein Scheunentor.

SRP können Viren stoppen, aber nicht den Nutzer.

Zum Lösen des Problems könnte man zwar UAC-Abfragen auch für die Benutzer-Ordner einbauen, doch dann wäre an sinnvolles Arbeiten kaum noch zu denken: Bei jedem Speichern und Zwischenspeichern von Dokumenten würde es Nachfragen hageln, ebenso bei jedem Kopiervorgang und bei jedem Löschen einer Datei und so weiter. Das würde also mehr Probleme verursachen als lösen.

Abhilfe SRP

Software Restriction Policies schützen anders: Sie sorgen dafür, dass Windows nur noch den Start zuvor festgelegter Anwendungen erlaubt. Als Folge kann sich ein Schädling zwar noch im Nutzerprofil einnisten, von dort aus aber nicht starten und somit keinen Schaden anrichten. Die Beschränkungen gelten dabei ausschließlich für ausführbare Dateien, also Dateitypen wie exe, bat, vbs und so weiter; die Liste ist anpassbar. Dokumente hingegen werden von SRP nicht überwacht: Das Öffnen von Texten, Tabellen, Videos et cetera ist also auch bei aktiven SRP problemlos möglich. Wichtig ist nur, dass die jeweils mit dem Dokumenten-Dateityp verknüpfte Anwendung erlaubt ist, beispielsweise das Office-Paket.

Es gibt verschiedene Arten von Regeln, die den Start von Programmen erlauben. Für einzelne ausführbare Dateien empfiehlt sich eine „Hash-Regel“. Beim Erstellen einer solchen Regel erzeugt Windows selbst einen Hash – eine Art einzigartiger Fingerabdruck – der Datei und gleicht künftig bei jedem Aufruf einer ausführbaren Datei ab, ob sie einen der erlaubten Hashes besitzt – nur dann wird sie ausgeführt. Dank des Hashes ist egal, an welchem Ort die Datei liegt und wie sie heißt, wichtig ist nur, dass sie unverändert ist. Ein Schädlingsbefall hingegen würde die Datei ändern, was zu einem nicht mehr passenden Hash führt.

Nun wäre es recht umständlich, für alle Programme, die man braucht, jeweils eine Hash-Regel zu erstellen. Deshalb gibt es einen weiteren Regeltyp: die Pfad-Regel. Damit ist gemeint, dass man per Regel den kompletten Inhalt eines Ordners mitsamt seiner Unterordner erlaubt. Sinnvoll ist das unter anderem bei den Ordnern „Windows“ und „Programme“ – ohne Ausnahmen für sie würde nicht nur keine der installierten Anwendungen mehr starten, sondern auch nicht mehr Windows selbst. Man würde stattdessen vor einem schwarzen Bildschirm sitzen. Daher erzeugt Windows Pfad-Regeln für diese beiden Ordner grundsätzlich von selbst beim Aktivieren des SRP-Mechanismus.

Beim Erstellen von Pfad-Regeln muss man aufpassen, dass man nur Pfade erlaubt, in denen Benutzer mit eingeschränkten Rechten keine Schreibrechte besitzen. Es gilt also, die Rechtekombination „Schreiben“ und „Ausführen“ zu verhindern. Denn in einem Ordner, in dem beides gleichzeitig erlaubt ist, kann sich ein Schädling wieder unbemerkt einnisten. Beim Programme-Ordner besitzt ein Nutzer mit eingeschränkten Rechten keinen Schreibzugriff, daher kann er problemlos einfach so als Pfad-Regel eingerichtet werden. Beim Windows-Ordner sieht es leider anders aus: In seinen Tiefen gibt es einzelne Unterordner, in denen Nutzer und Prozesse auch ohne Admin-

Rechte schreiben dürfen. Restric'tor bietet daher eine Option, solche Unterordner zu suchen und mit zusätzlichen Pfad-Regeln zu blockieren. Denn SRP können nicht nur erlauben, sondern auch verbieten. In verbotenen Ordnern können Sie einzelne Dateien trotzdem per Hash-Regel erlauben.

Bequem machen

SRP können nicht nur für Nutzer mit eingeschränkten Rechten gelten, sondern auch für Administrator-Konten. Davon ist aber im Normalfall abzuraten, denn das erschwert das Arbeiten unnötig: Wenn die SRP nur für Nutzer mit eingeschränkten Rechten gelten, können Sie bei Bedarf ein Programm per Rechtsklick „Als Administrator ausführen" und so beliebige Programme starten. Für Programme, die ohnehin Admin-Rechte brauchen, müssen die dann auch keine Regeln erstellen. Und falls der Abgabetermin mal wieder wichtiger als alles andere ist, können Sie so auch bei aktiven SRP mal eben das gerade lebensnotwendige Programm starten, selbst wenn es dafür noch keine Ausnahmeregel gibt.

Auch das Installieren von Anwendungen ist problemlos möglich: Starten Sie das Setup-Programm einfach als Admin. Wenn es die Anwendung korrekt in den Programme-Ordner installiert, brauchen Sie anschließend nicht mal eine neue Ausnahmeregel dafür zu erstellen.

Noteingänge

Software Restriction Policies schützen vor dem Start unerwünschter Anwendungen, aber wie jeder andere Schutzmechanismus kann das mitunter im falschen Moment passieren: Wenn die auf dem Desktop-PC erstellte Präsentation auf dem Notebook nicht starten will, weil das Office-Paket noch nicht erlaubt wurde, will man kaum vor den Augen des Chefs erst mit Regeln hantieren, sondern nur, dass es jetzt sofort geht. Kein Problem: Rechtsklick auf das Programm, „Als Administrator ausführen", läuft.

Falls es nicht um einen hektischen Einzelfall geht, sondern Sie sich beim Konfigurieren der Regeln verhaspelt haben, hilft Noteingang Nummer 2: Einfach alle Regeln löschen und von vorn anfangen. Falls selbst Restric'tor nicht mehr laufen sollte, löschen Sie mit regedit den kompletten Registry-Schlüssel `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\safer`. Schlimmstenfalls erledigen Sie das im abgesicherten Modus – da sind SRP grundsätzlich nicht aktiv. SRP können Sie von Ihrem Rechner daher nicht dauerhaft aussperren.

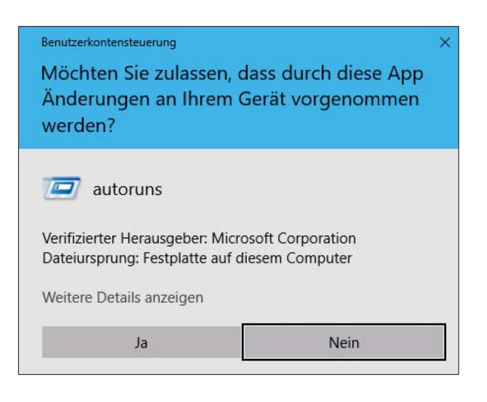
Nur mal gucken!

Wer nun wissen will, wie sich SRP auf dem eigenen Rechner auswirken, kann einen harmlosen Probelauf starten und lässt Windows in einer Log-Datei sämtliche Programmstarts protokollieren, die bei aktiven SRP von den Regeln überwacht worden wären. Auf diese Weise können Sie herausfinden, was SRP auf Ihrem Rechner bewirken würden, ohne sie dafür aktivieren zu müssen.

Dazu laden Sie sich unter ct.de/ym5g unser Programm „Restric'tor" herunter und starten es als Administrator. Im ersten Reiter ganz unten können Sie die Log-Datei erzeugen. Hangeln sie sich im „Durchsuchen"-Dialog zu einem beliebigen beschreibbaren Ordner durch, tippen Sie einen Dateinamen ins entsprechende Feld und klicken Sie auf Speichern. Nun noch auf „Anwenden" klicken, die Nachfrage bestätigen und schon erstellt Windows die Log-Datei. Lesen können Sie sie beispielsweise mit Notepad.

Die Log-Datei enthält keine persönlichen Informationen, sondern nur wenige Angaben zum jeweils protokollierten Ereignis: Jeder Eintrag beginnt mit dem Namen des auslösenden Prozesses, also beispielsweise svchost.exe beim Start von Diensten oder explorer.exe, wenn Sie selbst Anwendungen aus dem Startmenü oder eben aus dem Explorer starten. Es folgen die Prozess-ID (PID), Name und Pfad des gestarteten Programms sowie schließlich die ID jener Regel, die den Start erlaubt hat. Da Windows nicht mehr Informationen speichert und nur bei Programmstarts etwas in die Log-Datei schreibt, bleibt sie normalerweise auch nach Wochen wenige MByte klein.

Um sich einen Überblick zu verschaffen, wie viele Ausnahmeregeln zusätzlich zu den Standard-Regeln für den Windows- und den Programme-Ordner wohl



Solche Nachfragen mögen nerven, wenn man das fragliche Programm gerade selbst gestartet hat. Doch falls solche Nachfragen aus dem Nichts erscheinen, sind sie ein deutliches Alarmsignal.

nötig werden, nutzen Sie Ihren PC nach dem Aktivieren der Log-Datei einfach ein paar Tage wie gewohnt weiter. Danach schauen Sie in die Log-Datei. Tipp: Falls Sie sie zu unübersichtlich finden, kopieren Sie den kompletten Inhalt kurzerhand in eine Tabelle eines Office-Pakets und sortieren nach der Spalte mit den Pfadangaben. Interessant sind nur die Zeilen, in denen die Pfade anders beginnen als mit den genannten Ausnahmen „C:\Program Files" und „C:\Windows"; unter einem 64-bittigen Windows erfassen die Standard-Regeln zusätzlich den Ordner „C:\Program Files (x86)".

Bei unseren Tests passierte es mitunter, dass Windows bei tagelanger Laufzeit irgendwann das Protokollieren in der Log-Datei bis zum nächsten Neustart stoppte. Einen Grund dafür haben wir nicht finden können. Dramatisch ist das allerdings nicht, denn erstens reicht ein Neustart zum Lösen des Problems und zweitens gibt es weitere Optionen der Überwachung der SRP, die zuverlässig funktionieren – mehr dazu im Kasten auf Seite 86.

Änderungen durch SRP

Auch wenn alle Apps aus dem Store sowie die meisten herkömmlichen Programme problemlos bei aktivierter SRP laufen, muss man sich doch mitunter umgewöhnen. So erkennt Windows beispielsweise Programme, die Administratorrechte brauchen, entweder anhand einiger festgelegter Dateinamen wie setup.exe oder install.exe oder aber an einem in der Datei steckenden Manifest, welches die Rechte

anfordert. Die Überwachung durch die SRP schlägt aber in allen Fällen vorher zu und verhindert so das Anfordern und damit den Start des Programms. Auch hier hilft wieder, das Programm einfach per Rechtsklick und „Als Administrator ausführen“ zu starten. Sie erkennen solche Programme am kleinen Schild unten rechts im Programmsymbol.

Wer gern portable Anwendungen nutzt, die ohne Installation auskommen, kann das auch bei aktiven SRP. Für portable System-Utilities, die ohnehin nur mit Admin-Rechten laufen, sind nicht mal Regeln erforderlich. Für alle anderen erzeugt man kurzerhand Hash-Regeln. Problematisch werden nur portable Anwendungen, die gelegentlich oder gar häufig Updates brauchen, wie Browser oder Mail-Client. Hier müssten Sie dann jedes Mal die Regeln anpassen, und zwar sowohl für das Update-Programm als auch für das Programm selbst sowie gegebenenfalls für das Wrapper-Programm, das dafür sorgt, dass die Anwendung überhaupt portabel ist. Das ist nach unseren Erfahrungen auf Dauer nur was für Menschen mit sehr belastbarem Nervenkostüm. Wir empfehlen stattdessen, statt der portablen die installierbaren Versionen solcher Programme zu verwenden, denn im Programme-Ordner klappts auch mit dem Update.

In Einzelfällen kann es aber auch bei installierten Anwendungen zu Schwierigkeiten kommen. So lässt sich Googles Browser Chrome je nach Fassung wahlweise ins Nutzerprofil installieren, von wo aus er aber nur mit zusätzlichen Regeln laufen würde - die dank regelmäßiger Updates immer wieder anzupassen wären. Empfehlenswert ist hier, Chrome stattdessen in den Programme-Ordner zu installieren: Dann klappt alles inklusive Updates auch ohne zusätzliche Regeln. Noch etwas anders liegt der Fall bei Spotify: Der Client will sich grundsätzlich ins Benutzerprofil installieren, was dank ständiger Updates immer wieder eine Regel-Pflege erfordert. Doch auch hier gibt es Abhilfe: den Webplayer. Er läuft ganz ohne Ausnahmeregeln im Browser; Sie finden ihn unter play.spotify.com. Weitere Schwierigkeiten sind uns mit Electron-Apps wie Whatsapp aufgefallen, die ebenfalls im Benutzer-Ordner liegen, sowie mit Onedrive, Steam und Origin. Hier waren jeweils Ausnahmeregeln erforderlich.

Mitunter gibt es jedoch auch bei im Programme-Ordner installierten Anwendungen Schwierigkeiten beim Update. Der PDF-Viewer Foxit Reader beispielsweise erzeugt eine Updater.exe im Temp-Ordner des Benutzerprofils, doch von dort darf sie bei aktiver SRP nicht starten. Eine Pfad-Regel als Ausnahme hinzuzufügen verbietet sich, weil der Benutzer hier ja Schreibrechte hat. Abhilfe bringt hier, entweder für die updater.exe eine Hash-Regel zu erstellen, die dann aber immer dann aktualisiert werden muss, wenn auch updater.exe aktualisiert wurde, oder aber die automatischen Updates abzustellen und stattdessen gelegentlich den Reader als Administrator zu starten, um ihn Updates installieren zu lassen.

Beim Umgang mit Skripten muss man sich bei aktivierten SRP etwas umgewöhnen, denn als ausführbare Dateien unterliegen sie ja der SRP-Überwachung. Beispielsweise klappt bei Batch-Dateien ein Klick auf „Bearbeiten“ in deren Kontextmenü zum Öffnen mit Notepad nicht mehr. Sie können aber problemlos zuerst Notepad starten und das Skript dann über dessen Menü oder per Drag & Drop aus dem Explorer öffnen und bearbeiten. Das Ausführen des Skripts klappt dann aber wieder nur mit Administratorrechten oder nach dem Erstellen einer passenden Regel.

Die Windows PowerShell läuft bei aktiven SRP in einem „Constrained Language Mode“, in dem der Zugriff auf die meisten COM- und .NET-Objekte verboten ist. Gewöhnliche Cmdlets funktionieren aber wie gewohnt und in PowerShell-Sessions, die mit Administratorrechten gestartet wurden, ändert sich nichts. Details erläutert der Befehl `Get-Help about_Language_Modes`.

In der Log-Datei werden Ihnen auch immer wieder Einträge zu .lnk-Dateien auffallen, die Sie bei der Durchsicht aber einfach ignorieren können. Hier geht es nur um Verknüpfungen, die aus Sicherheitssicht völlig unkritisch sind, weil das Ziel der Verknüpfung ja ebenfalls von SRP überwacht wird – mehr dazu im nachfolgenden Artikel.

Und los ...

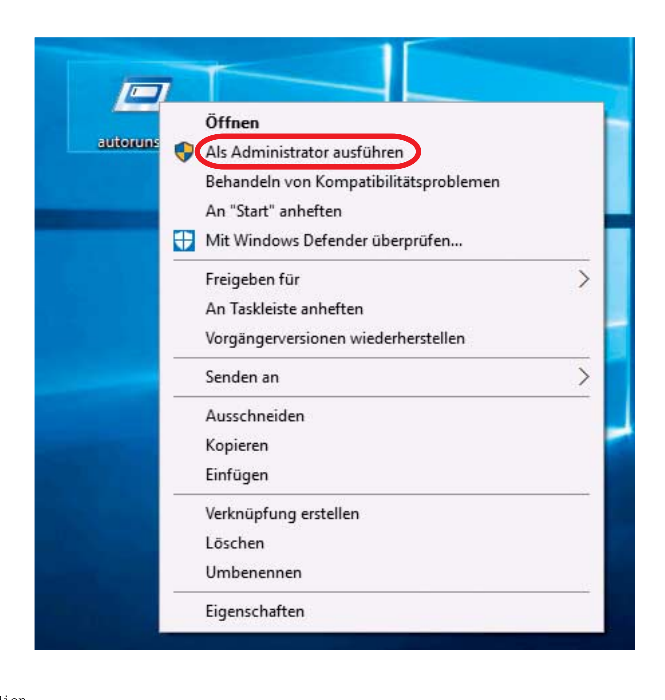
Nach dem Auswerten der Log-Datei können Sie sich entscheiden, auf welchen eigenen oder von Ihnen betreuten PCs Sie SRP aktivieren wollen. Wie genau das mit Restric’tor funktioniert, zeigt der nachfolgende Artikel. Er erläutert auch, wie Sie das Blockieren von Programmen möglichst bequem überwachen können.

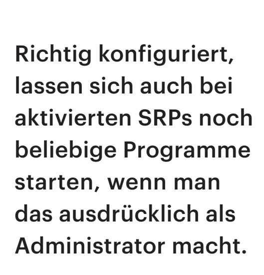
(axv@ct.de) **c't**

Literatur

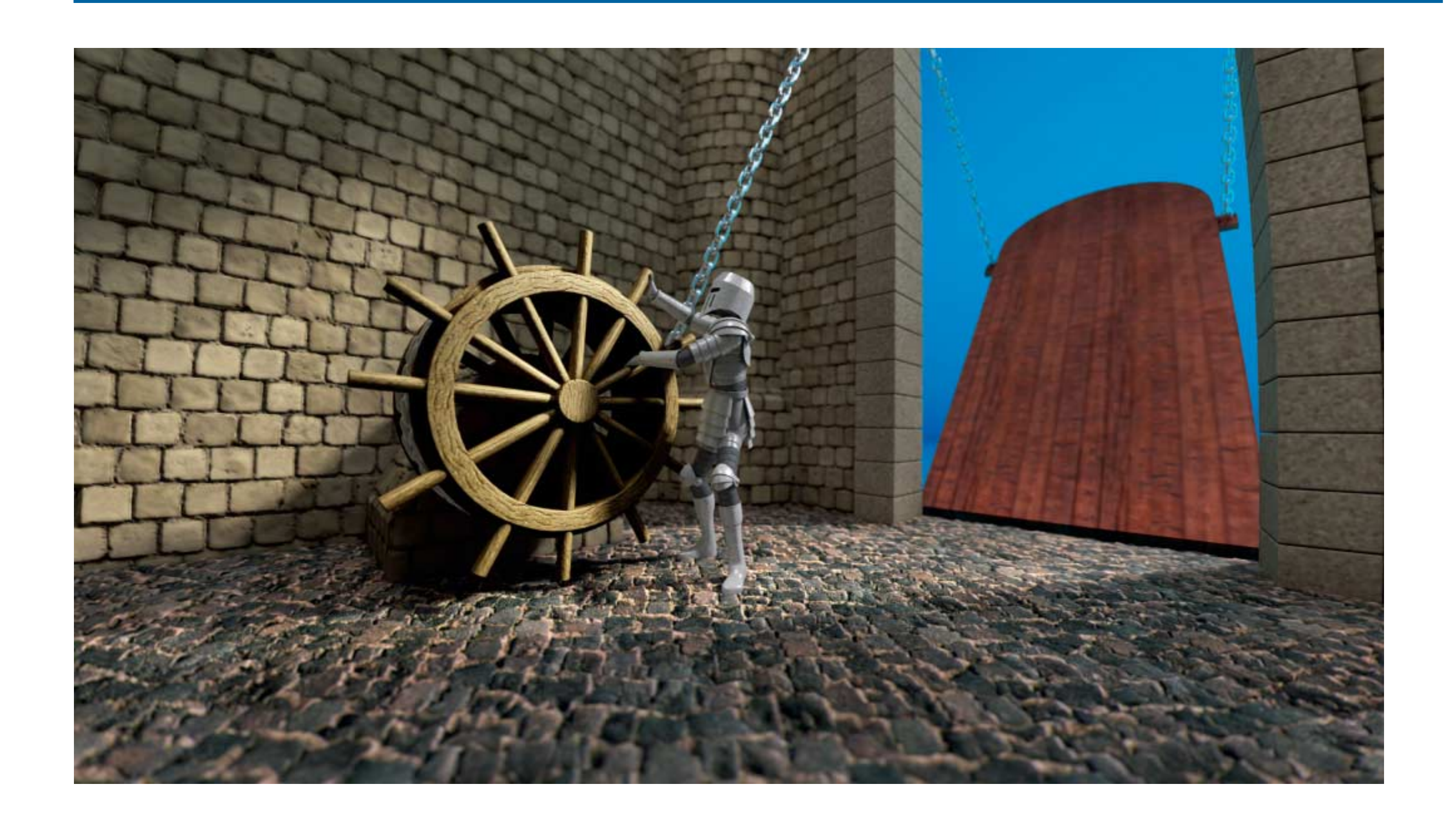
[1] Olivia von Westernhagen, Jürgen Schmidt, Die unsichtbare Gefahr, Dateilose Infektion umgeht Schutzfunktionen, c't 7/17, S. 96

Restric’tor: **ct.de/ym5g**





Richtig konfiguriert, lassen sich auch bei aktivierten SRPs noch beliebige Programme starten, wenn man das ausdrücklich als Administrator macht.



Schotten dicht!

Mit Restric’tor zum sicheren Windows

In die Windows-Ausgaben, die für den Einsatz in Unternehmen vorgesehen sind, baut Microsoft Funktionen ein, um sie zuverlässig vor Hacker-Angriffen zu schützen. Anwendern mit Windows Home bleibt der Zugang zu diesen Funktionen verwehrt – bislang: Mit dem c’t-Programm Restric’tor können Sie alle Windows-Editionen konfigurieren.

Von Hajo Schulz

Schadprogramme wie Viren oder Trojaner sind darauf angewiesen, Code auf dem Opfer-Rechner auszuführen. Um schädliche Programme auszusperren, scannt beispielsweise Antivirensoftware die Dateien auf der Festplatte und versucht, Code zu entdecken, der dem bereits bekannter Schädlinge ähnelt. Je nach dem Geschick der Entwickler gelingt ihr das mehr oder weniger erfolgreich.

Der perfekte Schutz eines idealen Systems bestünde wohl darin, es schlicht gar keinen Code mehr ausführen zu lassen, dessen Harmlosigkeit nicht zweifelsfrei belegt ist. Tatsächlich enthält Windows einen Mechanismus, mit dem man diesem Ziel sehr nahekommen kann: die „Richtlinien für Softwareeinschränkung“, englisch „Software Restriction Policies“ oder kurz SRP. Damit lassen sich Regeln definieren, die Windows anweisen, nur noch Programme aus einer zuvor festgelegten Liste auszuführen – unbekannter Code hat keine Chance mehr, Schaden anzurichten oder sich gar dauerhaft im System einzunisten.

Gedacht sind diese Richtlinien eigentlich dazu, dass Administratoren in Unternehmen den Katalog der erlaubten Anwendungen definieren und über Gruppenrichtlinien an alle Rechner in der Windows-Domäne verteilen. Werkzeuge zum Bearbeiten der Regeln bringen folgerichtig nur die für den Einsatz in Firmen vorgesehenen Professional-, Enterprise- und Ultimate-Ausgaben von Windows mit. Technisch sind diese Regeln aber nichts anderes als automatisch generierte Registry-Einträge. Wenn sie vorhanden sind, richtet sich auch ein Windows Home nach ihnen. Das nutzt unser Tool Restric’tor aus, das wir im Folgenden vorstellen: Es läuft unter allen Windows-Editionen seit Windows 7 und lässt Sie einigermaßen komfortabel die Registry-Schlüssel und -Werte der SRP bearbeiten.

Gibt es für Home-Anwender außer dem mühsamen und fehlerträchtigen Herumfrickeln direkt in der Registry kaum eine Alternative zu Restric’tor, müssen sich Pro- und Ultimate-Anwender entscheiden: Mit dem in ihrem Windows ent-

haltenen „Editor für lokale Gruppenrichtlinien“ (gpedit.msc) oder der „Lokalen Sicherheitsrichtlinie“ (secpol.msc) lassen sich in puncto SRP praktisch dieselben Einstellungen vornehmen wie mit Restric’tor. Hinter den Kulissen ist die Vorgehensweise aber eine komplett andere: Während Restric’tor direkt die zuständigen Registry-Einträge liest und schreibt, laden die Microsoft-Werkzeuge die Einstellungen zunächst in der lokalen Gruppenrichtlinie ab, von wo Windows sie beim Speichern und bei jedem Systemstart in die Registry übernimmt. Anders gesagt: Restric’tor stellt stets die aktuell gültigen Systemeinstellungen dar, während die Windows-eigenen Editoren eher indirekt arbeiten. Daher sollten Sie es vermeiden, mal dieses und mal jenes Tool zu verwenden – Verwirrung wäre programmiert. Um Richtlinien zum Verteilen in einer Domäne vorzubereiten, eignet sich Restric’tor nicht; hier sind die Windows-eigenen Werkzeuge alternativlos.

Den Restric’tor gibt es unter ct.de/y9wc zum Download. Für ein erstes Ausprobieren können Sie die EXE-Datei einfach in irgendeinen Ordner auf Ihrer Festplatte kopieren – auf eine sichere Installation für die regelmäßige Benutzung gehen wir weiter unten noch ein. Restric’tor erfordert ein installiertes .NET Framework ab Version 4.0; die Windows-Versionen ab Windows 8 haben alles Benötigte von vornherein an Bord, unter Windows 7 rüsten die „Empfohlenen Updates“ .NET 4.5 nach. Das Programm benötigt Administratorrechte.

Kennenlernen

Wenn Sie sich auf Ihrem PC noch nie mit Software Restriction Policies beschäftigt haben, wird auf der Seite „Allgemein“ von Restric’tor einzig die von Windows vorgegebene Option „Administratoren einschließen“ ausgewählt sein; die Liste der Regeln auf der zweiten Seite ist leer. Zu diesem Zustand (der Schutzlosigkeit) können Sie jederzeit zurückkehren, indem Sie im Menü den Befehl „Datei/SRP-Richtlinie komplett löschen“ wählen. Dies ist übrigens die einzige Aktion in Restric’tor, die sich sofort auf Ihr Windows auswirkt. Alle anderen Einstellungen, die Sie in dem Programm vornehmen, werden erst aktiv, nachdem Sie die Schaltfläche „Anwenden“ am unteren Fensterrand anklicken.

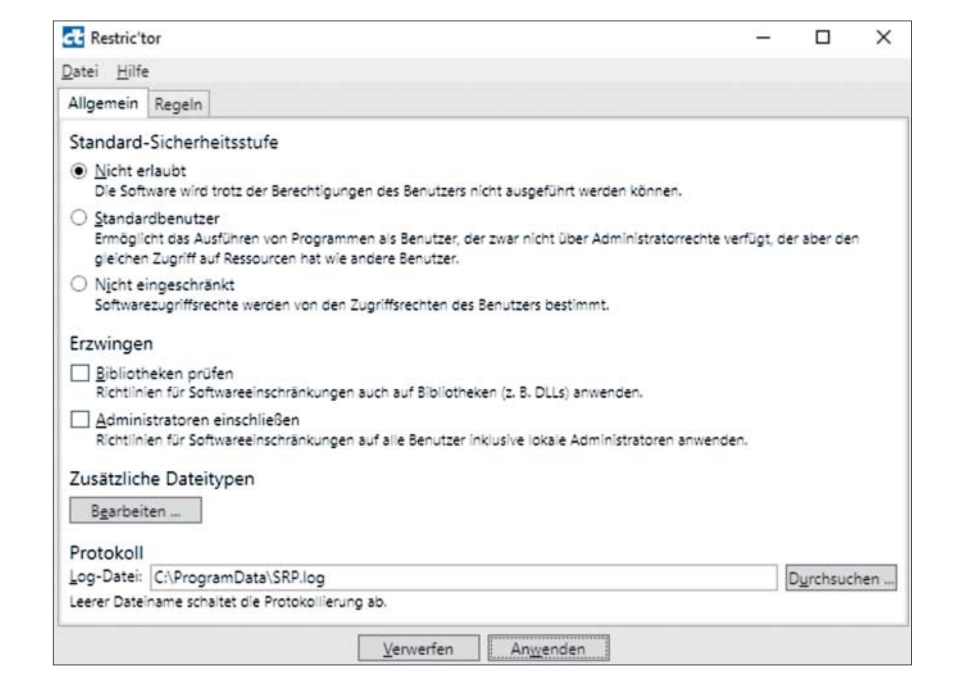
Sollten Sie sich mit den Optionen von Restric’tor mal versehentlich so verhaspelt haben, dass das Programm selbst sich nicht mehr starten lässt, können Sie die SRP direkt in der Registry zurücksetzen: Löschen Sie einfach den kompletten Schlüssel `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\safer`. Extrem experimentierfreudigen Naturen könnte es sogar gelingen, die SRP so zu konfigurieren, dass selbst das Programm regedit nicht mehr startet. Ihnen bleibt dann nur, Windows im abgesicherten Modus zu starten: Dort werden die Richtlinien nicht beachtet und der Registrierungs-Editor lässt sich auf jeden Fall benutzen.

Der Hauptschalter für die SRP besteht in Restric’tor aus den Optionen unter „Standard-Sicherheitsstufe“. „Nicht eingeschränkt“ entspricht dem Auslieferungszustand von Windows: Die passenden Benutzerrechte vorausgesetzt führt das Betriebssystem jedes Programm ungefiltert aus. Eingeschaltet wird die SRP-Prüfung mit „Nicht erlaubt“: Damit ist zunächst einmal die Ausführung sämtlicher Programme verboten – nicht einmal die EXE-Dateien, die zum Betriebssystem gehören, würden starten; Windows wäre ohne weitere Vorkehrungen unbenutzbar. Beim Klick auf „Anwenden“ prüft Restric’tor aber, ob so ein Zustand eintreten würde, und verweigert im Zweifel das Schreiben in die Registry mit einer Fehlermeldung.

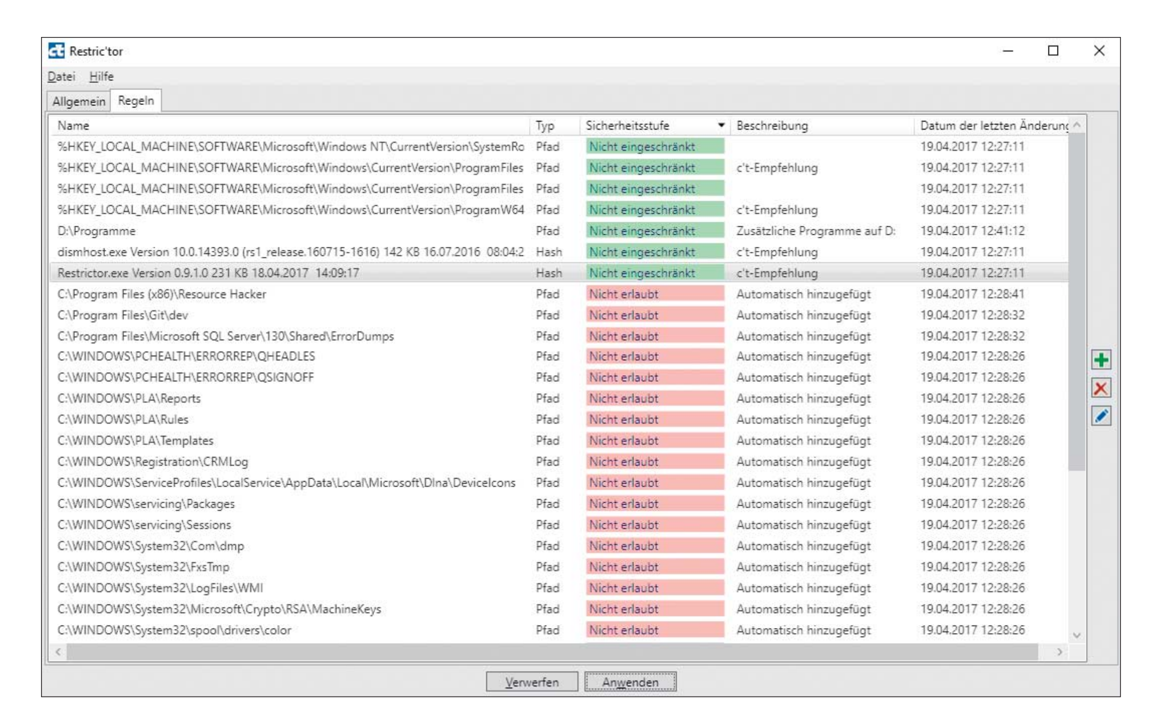
Die Option „Standardbenutzer“ hat eigentlich nur unter Windows Server eine Bedeutung und ist auf dem Desktop nicht zu empfehlen. Restric’tor bietet sie lediglich der Vollständigkeit halber an. Ihr Effekt entspricht im Wesentlichen der Einstellung „Nicht erlaubt“.

Der Schalter „Bibliotheken prüfen“ bringt zwar etwas zusätzliche Sicherheit, drückt aber sehr stark auf die Gesamt-Performance des Systems und ist deshalb nicht zu empfehlen. Er ist in Restric’tor eigentlich nur deshalb vorhanden, damit Sie ihn ausschalten können, falls er durch ein anderes Werkzeug aktiviert wurde.

Dasselbe gilt für die widersinnigerweise von Windows selbst aktivierte Vorgabe „Administratoren einschließen“. Damit sägen Sie unter Umständen den Ast ab, auf dem Sie sitzen: Wenn die anderen SRP-Optionen die Ausführung von Restric’tor nicht explizit erlauben, können Sie ihn (und alle anderen Programme) immer noch per Rechtsklick „Als Adminis-



Die wichtigsten Optionen zum Konfigurieren der Software Restriction Policies versammelt Restric’tor auf der ersten Seite. Die Standard-Sicherheitsstufe entscheidet darüber, ob sie überhaupt beim Laden von Programmen eingreifen.



Die zweite Seite von Restric'tor dient dazu, Regeln zu definieren, nach denen die SRP vertrauenswürdige Programme identifizieren. Ohne solche Regeln wäre der Rechner bei eingeschalteten SRP unbenutzbar.

trator starten". Der Schalter „Administratoren einschließen" verhindert das. Mit etwas Unachtsamkeit blockieren Sie so sogar den Registry-Editor und sind auf den abgesicherten Modus angewiesen, um die SRP anders zu konfigurieren.

Damit die Erlaubnis zum Ausführen von Programmen mit Administratorrechten nicht zu einem Loch wird, durch das sich doch wieder unbekannte und möglicherweise gefährliche Software in Ihr Windows einschleicht, sollten Sie in der Systemsteuerung unter „Sicherheit und Wartung" die „Einstellungen der Benutzerkontensteuerung" aufrufen. Schieben Sie den Regler für die Benachrichtigungen mindestens auf die zweite Stufe von oben, besser ganz hinauf. Sollte in der Folge eine der bekannten Sicherheitsabfragen der Benutzerkontensteuerung („Möchten Sie zulassen, dass durch diese App Änderungen an Ihrem Gerät vorgenommen werden?") aus dem Nichts auftauchen, ist das ein sicheres Zeichen dafür, dass irgendein Programm versucht, sich an den SRP vorbeizumogeln. Im Zweifel ist dann „Nein" die richtige Antwort.

Wie schon gesagt dienen die SRP dazu, das Laden von ausführbarem Code zu verhindern, der dem System schaden könnte. Code wird von Windows aber nur gestartet, wenn er in einer Datei steckt, die das System entweder als direkt ausführbar kennt oder die einem Programm zugeordnet ist, das seinerseits den enthaltenen Code ausführen kann. Die Dateitypen, die aus Sicht der SRP in die zweite Kategorie fallen, bestimmt die Liste, die sich in Restric'tor bei einem Klick auf „Bearbeiten" unter „Zusätzliche Dateitypen" öffnet. Um sie nicht von Hand füllen zu müssen, sollten Sie bei der Ersteinrichtung der SRP einen der Befehle „Microsoft-Standardwerte laden" oder besser „c't-Empfehlung laden" aus dem Datei-Menü in Restric'tor auswählen. Die Liste der überwachten Dateitypen unterscheidet sich bei beiden nur in einem Eintrag: .LNK-Dateien zu überwachen, wie Microsoft vorgibt, halten wir für überflüssig, denn eine Verknüpfung ist ja für sich alleine genommen nicht gefährlich, selbst wenn sie ein böses Programm anlegt. Entscheidend ist, dass das Ziel überwacht wird, auf das sie verweist – und darum kümmern sich die anderen SRP-Regeln.

Mit dem Eingabefeld „Log-Datei" können Sie Windows anweisen, sämtliche Programmstarts zu protokollieren. Jeder Eintrag vermerkt, ob die SRP das Programm zugelassen oder blockiert haben und welche Regel für die Entscheidung verwendet wurde. Das ist vor allem sinnvoll, um sich vor dem Scharfschalten der SRP zunächst einen Eindruck davon zu verschaffen, wo im laufenden Betrieb mit Hindernissen zu rechnen ist – siehe den vorangegangenen Artikel auf Seite 76.

Sind die SRP aktiv, gibt es einen besseren Weg, ihre Arbeit unter Beobachtung zu halten: Jedes Mal wenn sie einen Programmstart verhindern, schreibt Windows einen Eintrag in das System-Log, wo sich die Aktivitäten dann mit der Ereignisanzeige verfolgen oder mit geeigneten Werkzeugen automatisch auswerten lassen – siehe Textkasten auf Seite 86.

Regelkunde

Die eben schon erwähnten Restric'tor-Menübefehle zum Laden einer Grundkonfiguration initialisieren nicht nur die Liste der überwachten Dateitypen, sondern legen auch schon einige Regeln an, die in der Liste auf der gleichnamigen zweiten Seite erscheinen. Deren Notwendigkeit erschließt sich, wenn man sich vergegenwärtigt, wie die SRP funktionieren: Mit der Standard-Sicherheitsstufe „Nicht erlaubt" ist zunächst einmal das Ausführen sämtlicher Programme verboten. Damit Windows funktioniert und Sie vernünftig arbeiten können, muss es Ausnahmen geben – und genau die bestimmen Sie mit den Regeln.

Ziel der SRP ist es, nur noch Code zuzulassen, dem Sie vertrauen. Dieses Prädikat verdient zunächst einmal alles, was zu Windows selbst gehört, also der Inhalt des System-Ordners. Der heißt normalerweise C:\Windows, kann aber in Einzelfällen auch mal woanders liegen. Deshalb verweist die zuständige Regel nicht direkt auf C:\Windows, sondern über den Registry-Eintrag `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SystemRoot`. Ähnliches gilt für die Ordner „Programme" und „Programme (x86)", in die Sie normalerweise Anwendungen installieren.

All diesen Ordnern ist gemeinsam, dass dort nur Prozesse schreiben dürfen, die mit Administrator- oder Systemrechten laufen: im Systemordner etwa Windows Update und in den Programmver-

zeichnissen Setup-Programme, die Sie ausdrücklich mit Administratorrechten gestartet haben. Sofern Sie die Sicherheitsabfragen der Benutzerkontensteuerung ernst nehmen, enthalten diese Ordner also nur Code, dem Sie schon einmal explizit vertraut haben.

Pfad-Regeln mit der Sicherheitsstufe „Nicht eingeschränkt“ sind also dazu da, Ordner zu identifizieren, in denen vertrauenswürdiger Code liegt. Damit diese Eigenschaft erhalten bleibt, sollten Sie auf keinen Fall an den Rechten dieser Ordner herumdoktern und normalen Benutzern Schreibzugriff gewähren. Das wäre dann nämlich genau das Einfallstor, auf das die Programmierer etwa von Erpressungstrojanern warten: Ein unbedacht angeklickter Mail-Anhang oder ein Dokument mit versteckten Makros könnte dort Code abladen und sich so ins System einnisten.

Wenn Sie diesen Grundsatz beachten, können Sie in Restric’tor selbstverständlich auch weitere Pfad-Regeln mit der Sicherheitsstufe „Nicht eingeschränkt“ anlegen: Der „+“-Knopf neben der Regelliste bringt ein Menü zum Vorschein, in dem sich unter anderem der Befehl „Neue Pfad-Regel“ findet.

In Frage kommt zum Beispiel ein Ordner auf einem anderen als dem Systemlaufwerk, in den Sie gelegentlich Programme installieren, etwa um den Platz auf der knapp bemessenen System-SSD zu schonen. Dann sollten Sie in diesem Ordner aber auch normalen Benutzern die Schreibrechte entziehen. Bewährt hat sich, in so einem Ordner dieselben Rechte zu vergeben, die auch im standardmäßigen Programme-Ordner gelten. Am einfachsten erreichen Sie das, indem Sie dessen Rechte kopieren, zum Beispiel mit der Befehlsfolge

```
$acl = Get-Acl "C:\Program Files"
Set-Acl "D:\Programme" $acl
```

Eingeben müssen Sie diese Kommandos in eine mit Administratorrechten gestartete PowerShell; in der zweiten Zeile ist der Name des Zielordners gegebenenfalls anzupassen.

Ausnahme von der Ausnahme

Leider enthält schon der Systemordner einer frischen Windows-Installation einige Verzeichnisse, in die man mit eingeschränkten Benutzerrechten schreiben kann. Auch im Programme-Ordner sind uns auf einigen Rechnern von Benutzern beschreibbare Verzeichnisse untergekommen – unverantwortlicherweise stammten auch die offenbar von Installationen von Microsoft-Programmen. Die Rechte dieser Ordner einzuschränken, damit sich dort keine Malware breit machen kann, ist al-



lerdings keine gute Idee, denn das könnte die Funktion der betroffenen Programme beeinträchtigen. Vielmehr sollte man die SRP so konfigurieren, dass das Ausführen von Programmen aus diesen Verzeichnissen verboten ist. Dafür sind Ordnerregeln mit der Sicherheitsstufe „Nicht erlaubt“ gedacht. Um solche Ordner zu identifizieren, enthält Restric’tor den Menübefehl „Datei/Ordner prüfen“. Auf dem Dialog, den er auf den Plan ruft, klicken Sie einfach die Schaltfläche „Ordner suchen“ an. Daraufhin prüft Restric’tor die Rechte in den Unterverzeichnissen sämtlicher Ordner, für die eine „Nicht eingeschränkt“-Ordnerregel konfiguriert ist. Alle Ordner, in die Sie ohne Administratorrechte schreiben dürfen, zeigt er in der Liste auf dem Dialog an. Ein Klick auf OK erzeugt für jeden Eintrag, bei dem Sie nicht das Häkchen entfernt haben, eine Ordnerregel der Sicherheitsstufe „Nicht erlaubt“.

Extrawurst

Auf den meisten Windows-Rechnern finden sich auch außerhalb der Windows- und Programme-Ordner Programme, auf die der Anwender nicht verzichten möchte: Auf die Schnelle heruntergeladene Spezialwerkzeuge ohne eigenes Installationsprogramm gehören ebenso in diese Kategorie wie portable Anwendungen, die man etwa auf einem USB-Stick mit sich herumträgt.

Für die erste Sorte empfehlen wir, einen Unterordner – etwa „Tools“ – im Programme-Ordner anzulegen. Um die Utilities dort abzulegen, braucht man dann einen Dateimanager, den man mit

Reagieren auf SRP-Ereignisse

Von Peter Siering

Wenn eine Software Restriction Policy das Ausführen eines Programms verhindert, notiert Windows ein Event im Ereignisprotokoll für Anwendungen. Die Wichtigkeit stuft das Betriebssystem als Warnung ein, womit die Ereignisse selbst aufmerksamen Betrachtern dieser zentralen Protokollinstanz entgehen dürften. Man muss schon explizit danach suchen, um sie im Wust der von Windows dort notierten Dinge zu finden.

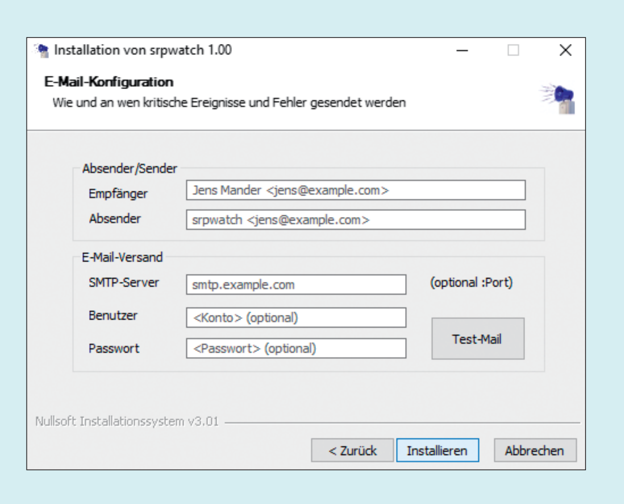
Einfach gelingt die Suche in der Ereignisanzeige über einen Filter, der die Quelle „SoftwareRestrictionPolicies“ auswählt. So erwischt man alle Ereignisarten, auch wenn bei unseren Experimenten nur wenige überhaupt auftreten, die sich darin unterscheiden, welche Art von Richtlinie die Ausführung eines Programms verhindert hat.

Nützlich sind sie durchaus: Einen – meist schnell weggeklickten – Dialog bekommt der Anwender bei einem SRP-Treffer nur zu sehen, wenn er den Programmstart selbst veranlasst hat; Autostarts und geplante Aufgaben scheitern stillschweigend. Im Unterschied dazu werden die Ereignisse im System-Log in jedem Fall erfasst und lassen sich auch später noch nachlesen und vor allem weiterverarbeiten. Letzteres könnte in einer Management-Lösung geschehen, die alle PCs im Netz im Auge behält, oder in kleinerem Rahmen, um Kenntnis eventueller SRP-Treffer auf einem entfernt stationierten PC zu erhalten.

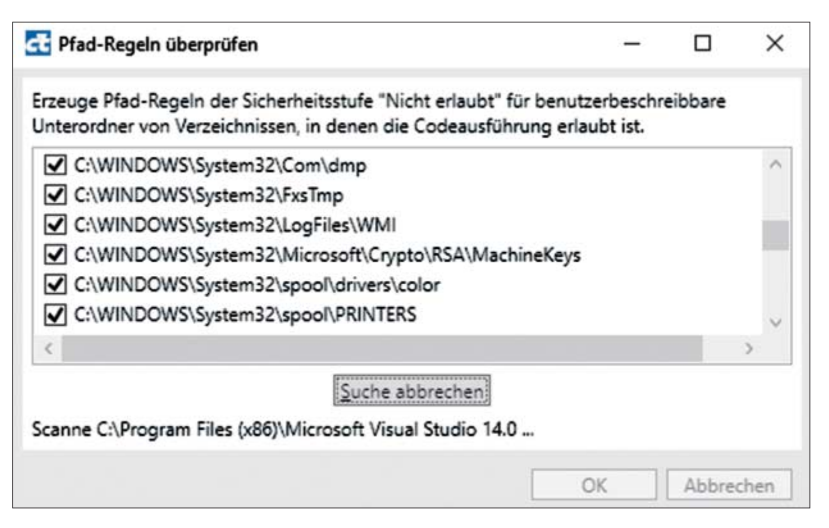
Aus unserer Sicht gut dafür geeignet ist E-Mail, die idealerweise nicht demjenigen zugeht, der den betroffenen PC benutzt, sondern dem, der ihn verwaltet. So lag es nahe, unser in [1, 2] vorgestelltes EventWatch-Projekt für dieses Nutzungsszenario umzubauen: Das dabei herausgekommene SrpWatch funktioniert ähnlich, hat sich aber auf die SRP-eigenen Ereignisse spezialisiert.

SrpWatch lauscht über eine geplante Aufgabe am Ereignisprotokoll. Wenn ein Eintrag mit der oben genannten Quelle ins Anwendungs-Log gerät, läuft das PowerShell-Skript an: Es sendet dann die seit dem letzten Lauf hinzugekommenen Einträge per E-Mail an eine beim Einrichten vorgegebene Adresse. Damit bei akutem Trojanerbefall das Konto nicht geflutet wird, läuft das Skript maximal alle fünf Minuten. In der Zwischenzeit aufgelaufene Ereignisse landen dann gebündelt in einer Nachricht.

Die Installation von SrpWatch müssen Sie nicht wie anfangs die von EventWatch zu Fuß erledigen. Das über den Download-Link (ct.de/y9wc) erhältliche Installationspaket erledigt alles: Es packt die Dateien in die für Programme vorgesehenen Verzeichnisse, fragt die E-Mail-Konfiguration ab, testet sie auf Wunsch und richtet die geplanten Aufgaben ein. Bei der Deinstallation verschwindet all das wieder aus dem System.



Unser Tool SrpWatch lauscht am Ereignisprotokoll für die SRP und benachrichtigt Sie per E-Mail, wenn eine Regel ein Programm blockiert hat. Die Einrichtung erledigt eine eigene Installationsroutine.



Unverständlicherweise lässt Microsoft zu, dass normale Benutzer in einigen Unterverzeichnissen des Systemordners Schreibzugriff haben. Restric'tor hilft dabei, sie zu finden und zu sperren.

Administratorrechten starten kann. Der Favorit des Autors dieser Zeilen heißt Double Commander, als Notnagel kann auch der „Datei öffnen"-Dialog eines mit Administratorrechten gestarteten Notepad herhalten. Ein solcher Tools-Ordner ist übrigens auch der empfohlene Speicherort für den Restric'tor.

Dieses Vorgehen funktioniert allerdings für die meisten portablen Anwendungen nicht: Sie benötigen in ihrem eigenen Ordner Schreibrechte, auch wenn sie unter einem eingeschränkten Benutzerkonto laufen. Den Ordner zu verrammeln scheidet also ebenso aus, wie in ihm enthaltenen Code per SRP-Pfad-Regel zu erlauben. Letzteres ist für Verzeichnisse auf USB-Sticks ohnehin keine gute Idee: Die meisten Sticks sind mit dem Dateisystem FAT32 formatiert. Das kennt aber keine Rechteverwaltung, sodass Benutzerprozesse generell überall schreiben dürfen – ein ideales Einfallstor für Schädlinge.

Für solche Fälle kennen die SRP Hash-Regeln: Mit ihnen identifiziert man jeweils eine einzelne ausführbare Datei als vertrauenswürdig. Entscheidend sind dabei nicht Merkmale wie Dateipfad, -größe oder Änderungsdatum, sondern eben ein Hash, also ein digitaler Fingerabdruck der Datei. Das hat den Vorteil, dass eine Malware keine Chance hat, sich beispielsweise in ein erlaubtes Programm hineinzukopieren: Sie würde den Hash dabei unweigerlich verändern. Weil den Hash-Regeln der Speicherort der Datei egal ist, funktionieren sie außerdem auch, wenn der Stick mit den portablen Programmen mal einen anderen Laufwerksbuchstaben zugewiesen bekommt.

Der Vorteil, Dateien unverwechselbar zu identifizieren, wird allerdings zum Nachteil, wenn die betroffene Anwendung häufig Updates erhält: Dann muss man jedes Mal den Hash neu berechnen, um das Programm wieder zuzulassen. Problematisch sind auch Programme, die sich in einen von Benutzern beschreibbaren Ordner installieren, um sich stillschweigend und ohne Sicherheitsabfrage aktualisieren zu können: Wenn die SRP plötzlich melden, dass sie so ein Programm blockiert haben, muss man als verantwortungsvoller Anwender eigentlich jedes Mal prüfen, ob sich der Hash durch ein legitimes Update geändert hat oder womöglich doch ein Trojaner eingedrungen ist. Wie das mit wenig Aufwand gelingt, erklärt der nachfolgende Artikel.

In Restric'tor legt man eine neue Hash-Regel über den „+"-Knopf neben der Regelliste und Auswahl von „Neue Hash-Regel" an. Über die „Durchsuchen"-Schaltfläche navigiert man zu der gewünschten Programmdatei. Die Dateiinformationen, die Restric'tor daraufhin in das zuständige Feld einträgt, dienen nur dazu, die Regel später in der Liste wiederzufinden. Den Hash berechnet das Programm im Hintergrund – es handelt sich um eine mehr oder weniger zufällige, nichtssagende Zeichenfolge. Um eine Hash-Regel etwa nach einem Update des betroffenen Programms zu aktualisieren, rufen Sie sie per Doppelklick oder über den Stift-Knopf neben der Regelliste auf und wiederholen die Auswahl der Programmdatei. Löschen lassen sich Pfad- und Hash-Regeln mit dem roten X neben der Regelliste.

Falls Sie sich wundern, warum die Regelliste nach dem Laden der c't-Empfehlungen bereits zwei Hash-Regeln enthält: Mit der einen kennzeichnet sich der Restric'tor selbst als vertrauenswürdig. Nach einem eventuellen Update von Restric'tor können Sie das mit dem Menübefehl „Datei/Hash-Regel für Restric'tor hinzufügen" wiederholen. Die zweite betrifft eine Windows-eigene Datei namens dismhost.exe, die partout aus dem Nutzer-Ordner starten will. Hintergrund ist eine systemeigene geplante Aufgabe, die gelegentlich prüft, ob noch ausreichend Platz auf der Platte frei ist. Da Windows dismhost.exe aber jedes Mal aus dem Windows-Ordner dorthin kopiert und nach dem Ende der Aufgabe wieder löscht, erfasst die Pfad-Regel für den Systemordner diese Aktion nicht.

Sonst noch

Wie eingangs erwähnt, eignet sich Restric'tor nicht, um Software Restriction Policies in einem Firmennetz auszurollen. Im privaten Rechnerzoo mag aber durchaus der Wunsch aufkommen, einen mühsam erstellten Regelsatz von einer Maschine auf eine andere zu übertragen. Dazu dienen die Befehle „Konfiguration exportieren" und „Konfiguration importieren" aus dem Datei-Menü. Sie leisten auch gute Dienste, um die SRP-Konfiguration vor einer geplanten Neuinstallation des Betriebssystems in Sicherheit zu bringen.

Unter ct.de/y9wc finden Sie außer dem Download des Programms ein Diskussionsforum, in dem Sie sich mit anderen Benutzern über Erfahrungen mit dem Tool austauschen können. Außerdem halten wir Sie auf der Projektseite über mögliche Updates von Restric'tor und SrpWatch auf dem Laufenden.

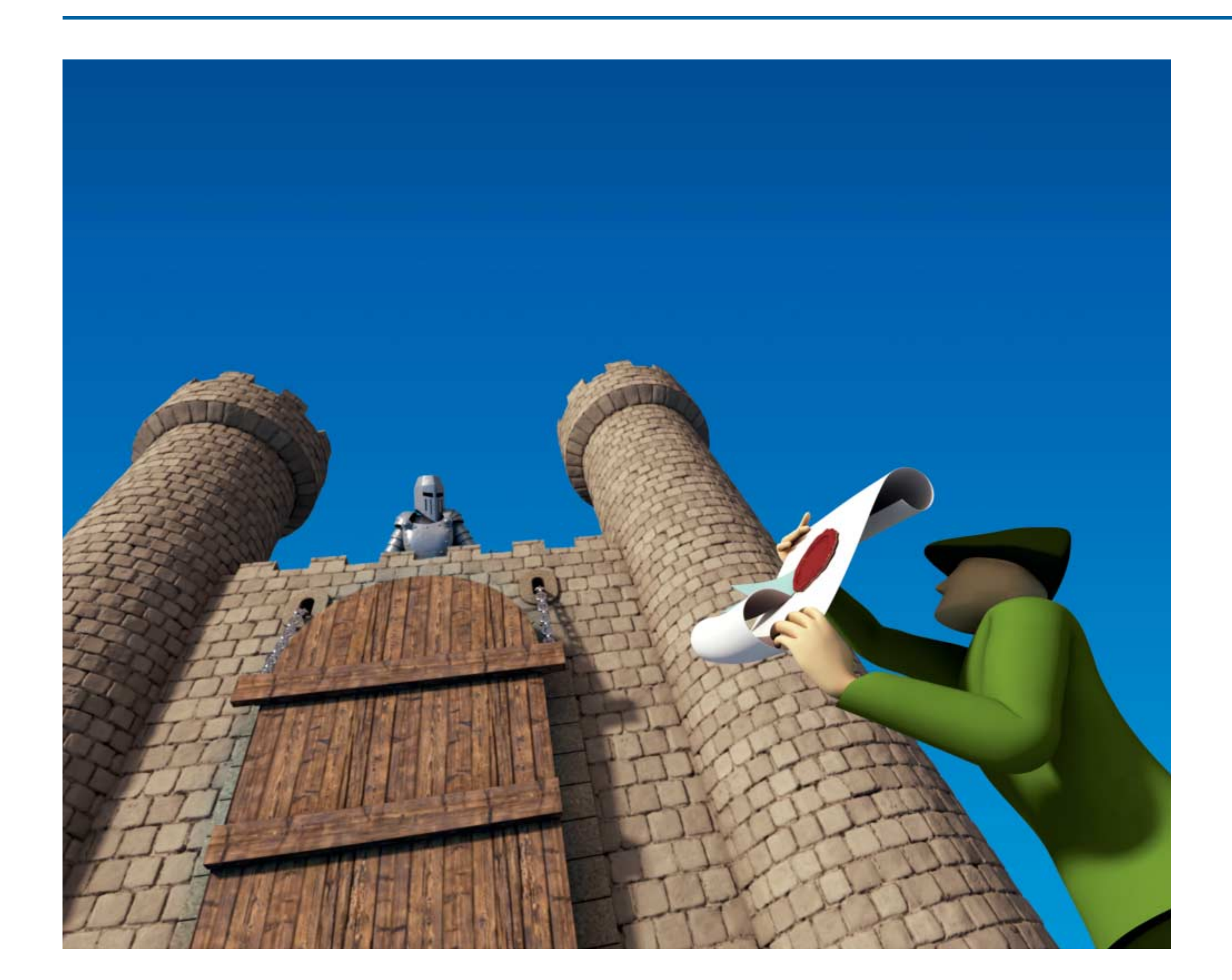
(hos@ct.de) c't

Literatur

[1] Peter Siering, Selbstüberwachung, Ereignisprotokolle im Blick, c't 10/12, S. 148

[2] Peter Siering, Pakete schnüren, Installer für Windows-Programme oder -Skripte, c't 16/14, S. 164

***Projektseiten zu Restric'tor und SrpWatch:* ct.de/y9wc**



Einlasskontrolle

Einschätzen, ob man einer Datei besser misstrauen sollte

Da liegt sie nun im Download-Ordner, die frisch heruntergeladene ausführbare Datei. Doch ist ein Doppelklick darauf womöglich gefährlich? Für eine erste Einschätzung reichen Sekunden.

Von Axel Vahldiek

Bei einer frisch heruntergeladenen oder per Mail empfangenen Datei besteht immer ein gewisses Risiko, dass sie einen Schädling enthält. Und das gilt keineswegs nur für Dateien aus dubiosen Quellen, sondern auch für Dateien von seriösen Anbietern oder Absendern, etwa weil sie selbst Opfer eines Angriffs wurden. Doch wie prüft man so eine Datei? In unseren „Analysiert“-Artikeln haben wir exemplarisch gezeigt, wie viel Aufwand Profis in gründliche Untersuchungen stecken [1, 2]. Einen ersten Eindruck bekommen Sie jedoch auch ohne Expertenwissen und in Sekundenschnelle. Mit den Tipps aus diesem Artikel prüfen Sie nicht nur die Signatur mit einem einzigen Mausklick, sondern lassen die Datei auch noch zugleich von über 60 Virenscannern untersuchen.

Um aber eines noch mal in aller Deutlichkeit zu sagen: Die nachfolgend vorgestellte Methode zur Schnellprüfung stellt keineswegs sicher, dass eine Datei

wirklich unschädlich ist. Stellen Sie sich das ähnlich wie eine Fußgängerampel vor: Wenn es dumm läuft, können Sie auch bei Grün überfahren werden. Doch wenn die Ampel rot leuchtet, wissen Sie, dass sie stehenbleiben beziehungsweise in diesem Fall eben bloß nicht doppelklicken sollten.

Das Werkzeug

Möglich macht das Ganze die Freeware Sigcheck von Sysinternals. Autor ist Mark Russinovich, der auch die bekannten Systemwerkzeuge Autoruns, Process Explorer und Process Monitor geschrieben hat und seit vielen Jahren für Microsoft arbeitet. Sie finden das wenige hundert KByte kleine Programm zusammen mit allen anderen Sysinternals-Tools unter https://live.sysinternals.com. Sigcheck.exe bietet kein GUI, ist also ein reines Kommandozeilenprogramm. Das Folgende beschreibt zuerst die Optionen und Möglichkeiten von Sigcheck und anschließend, wie Sie die Prüfung mit Sigcheck so konfigurieren, dass künftig ein simpler Mausklick reicht.

Sigcheck war ursprünglich nur zum Prüfen der Signatur von Dateien gedacht, genauer, ob das als Signatur dienende Zertifikat von einer Zertifizierungsstelle ausgestellt wurde, der Windows vertraut. Das muss nicht direkt sein, sondern kann über mehrere andere vertrauenswürdige Zertifikate hinweg erfolgen: Zertifizierungsstelle A vertraut Zertifizierungsstelle B, die wiederum Zertifizierungsstelle C und so weiter („Zertifizierungskette“). Eine gültige Signatur hinterlegt der Hersteller als Nachweis in der Datei, dass sie wirklich von ihm stammt und dass er dazu steht. Über die Fehlerfreiheit oder Ungefährlichkeit einer Anwendung sagt die Signatur damit zwar nichts aus, doch Sie wissen dann, an wen Sie sich bei Problemen wenden können. Und Hersteller von Programmen mit gültigen Signaturen bemühen sich üblicherweise schon aus Angst vor einem Image-Schaden, dass ihre Programme möglichst fehlerfrei und ungefährlich sind.

Die Signatur ist an genau diese Datei gebunden, wird also ungültig, wenn sich auch nur ein Bit davon ändert. Sofern Sigcheck also ausgibt, dass eine Datei von Microsoft signiert wurde, können Sie ziemlich sicher sein, dass das auch so ist – nur „ziemlich“ sicher, weil es leider in Einzelfällen vorkommt, dass die Signatur gefälscht oder gestohlen ist. Das ist aber sehr aufwendig, sodass momentan die meisten Angreifer das unterlassen.

Seit einiger Zeit kann Sigcheck noch etwas anderes: Virustotal.com befragen. Diese Website wird von Google betrieben. Wenn man dort eine Datei hochlädt, wird sie von über 60 Virenscannern geprüft. Das Ergebnis der Virustotal-Abfrage durch Sigcheck bekommen Sie üblicherweise bereits nach Sekunden, weil das Programm im ersten Anlauf nicht die ganze Datei, sondern bloß einen Hash hochlädt.

Einrichten

Damit Sie nicht für jeden Sigcheck-Aufruf lange Kommandozeilenbefehle eintippen müssen, finden Sie unter ct.de/y8bm die Batch-Datei sigcheck.bat, die den Job für Sie erledigt. Laden Sie diese sowie sigcheck.exe herunter und packen Sie beide gemeinsam in einen beliebigen Ordner. Als Nächstes klicken Sie im Kontextmenü der Batchdatei sigcheck.bat auf „Kopieren“. Drücken Sie nun die Tastenkombination Windows+R, es öffnet sich der „Ausführen“-Dialog. Dort tippen Sie ein:

```
shell:sendto
```

Nach dem Bestätigen mit Enter öffnet sich der Ordner, in dem die Verknüpfungen des „Senden an“-Menüs aus dem Kontextmenü von Dateien und Ordnern liegen. Dort rechtsklicken Sie in einen leeren Bereich und wählen „Verknüpfung einfügen“ – fertig. Wenn Sie mögen, können Sie die Verknüpfung nach Gusto umbenennen.

Ab sofort können Sie jede Datei per „Senden an“-Menü an Sigcheck übergeben und bekommen anschließend ein Kommandozeilenfenster mit den Prüfungsergebnissen. Beim ersten Aufruf müssen Sie einmalig die Lizenzbestimmungen von Sysinternals sowie von Virustotal.com abnicken, ab dem zweiten Aufruf geht es ohne.

Wie Sigcheck genau vorgeht, können Sie konfigurieren. Dazu öffnen Sie die Batch-Datei im Texteditor. Die einzig relevante Zeile ist die zweite, sie lautet:

```
sigcheck.exe -vr -h %1
```

Die Option `-vr` sorgt dafür, dass der Hash der zu überprüfenden Datei bei Virustotal.com hochgeladen und dass die Ergebnisseite im Standardbrowser angezeigt wird, sofern mindestens ein Virenscanner Alarm schlägt. Finden alle Scanner die Datei harmlos, erscheint nur das Prüfergebnis im Kommandozeilenfenster. Wenn Sie wollen, können Sie die Option ergänzen zu `-vrs`. Das ist für den Fall gedacht, dass Virustotal den hochgeladenen Hash-Wert nicht erkennt, dann lädt Sig-

```
C:\WINDOWS\system32\cmd.exe
m:\progs\sysinternals\autoruns.exe:
        Verified:       Signed
        Signing date:   16:48 19.07.2016
        Publisher:      Microsoft Corporation
        Company:        Sysinternals - www.sysinternals.com
        Description:    Autostart program viewer
        Product:        Sysinternals autoruns
        Prod version:   13.62
        File version:   13.62
        MachineType:    32-bit
        MD5:    088E659223761E033284CE23CABFF819
        SHA1:   D6CF3A9028C3E8A47C97E57FBBA93157DC19AACC
        PESHA1: 9FA968EB40938E20657E34079F8F473E7CDC59A2
        PE256:  1E408BBC420589B0A7FD6648AC89D8D13D73869D4E3BAAAA9800F8AF29036187
        SHA256: FE7D78B9CCAF689785740E14E64A6B1B551667F82CAF3CE4FF236E7BA61EDE90
        IMP:    89FB6166114772C2C3B8139FACC129C9
        VT detection:   0/58
        VT link:        https://www.virustotal.com/file/fe7d78b9ccaf689785740e14e64a6b1b551667f82caf3ce4ff236e7ba61ede90/analysis/
Drücken Sie eine beliebige Taste . . .
```

Unser Skript bereitet seine Ausgabe zwar nicht gerade hübsch auf, informiert Sie aber in Sekundenschnelle darüber, ob eine Anwendung signiert ist und was über 60 Virenscanner darüber denken.

```
Auswählen C:\WINDOWS\system32\cmd.exe
f:\61327b698a626b760568ea37b026dfc3c684ee70d431348f363ea1c633e68999.exe:
        Verified:       Signed
        Signing date:   04:58 29.03.2017
        Publisher:      Nguyen Hoang Tung
        Company:        n/a
        Description:    n/a
        Product:        n/a
        Prod version:   1.3.0.0
        File version:   1.3.0.0
        MachineType:    32-bit
        MD5:    78ADC6AC4CF7A51F7DA68A06ACAC09E9
        SHA1:   39B089A559F8F4B5BD202EB2696D760428193D33
        PESHA1: 770B2A592645D6C34EA77BB67FB5BC5BB0367D49
        PE256:  C969F9DAC6C60FFC25EC255CB29F4679D3F1C557C1C3FA724E624683C35426FD
        SHA256: 61327B698A626B760568EA37B026DFC3C684EE70D431348F363EA1C633E68999
        IMP:    F34D5F2[illegible]D6D9CEEC516C1F5A744
        VT detection:   30/61
        VT link:        https://www.virustotal.com/file/61327b698a626b760568ea37b026dfc3c684ee70d431348f363ea1c633e68999/analysis/
Drücken Sie eine beliebige Taste . . .
```

Eine gültige Signatur weist zwar normalerweise darauf hin, dass eine Datei vertrauenswürdig ist, doch gibt es auch Ausnahmen. In diesem Fall schlagen gleich reihenweise Virenscanner Alarm, womit trotz gültiger Signatur klar ist: bloß kein Doppelklick auf die geprüfte Datei!

check die Datei selbst automatisch zur weiteren Prüfung hoch.

Wenn Sigcheck die komplette Zertifikatskette ausgeben soll, ergänzen Sie hinter `-vr` die Option `-i`. Dadurch wird die Ausgabe allerdings erheblich länger und damit unübersichtlicher.

Die Option `-h` lässt Sigcheck zusätzlich verschiedene Hash-Werte für die untersuchte Datei ausgeben (MD5, SHA256, ...). Für eine Prüfung auf Vertrauenswürdigkeit ist das eigentlich nicht erforderlich, spart aber in manch anderen Situationen ein zusätzliches Hash-Programm – falls Sie das nicht brauchen, streichen Sie die Option einfach. Das `%1` am Ende ist keine Option, sondern eine hier unverzichtbare Variable, die für die an die Batch-Datei übergebene Datei steht.

Ausgabe

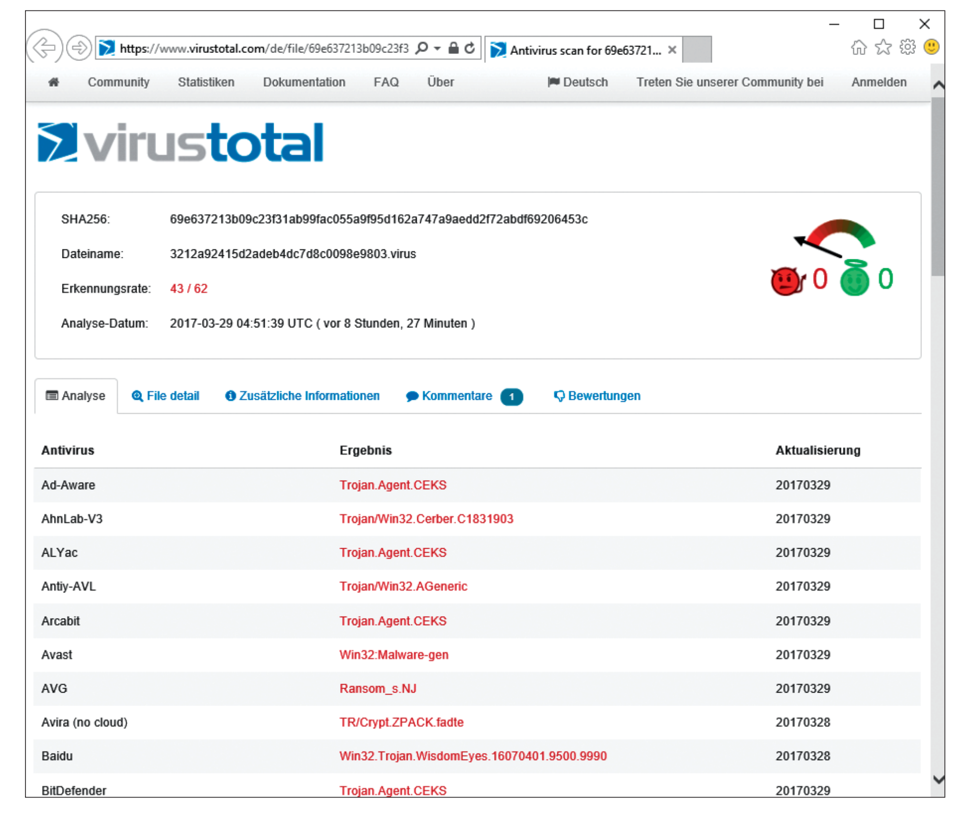
Die Ausgabe des Skripts im Kommandozeilenfenster verdient zugegebenermaßen keinen Schönheitspreis, sondern fasst einfach nur in drögen Textzeilen und zum Teil mit Abkürzungen die Ergebnisse zusammen.

Die erste Zeile beginnt mit „Verified“, dahinter steht normalerweise entweder „Signed“ oder „Unsigned“. Zumindest bei großen Firmen wie Microsoft und Google sollte die Datei grundsätzlich signiert sein, auch wenn Ausnahmen die Regel bestätigen.

In manchen Fällen ist zwar eine Signatur vorhanden, wird aber nicht als vertrauenswürdig eingestuft. Sie erkennen das an Meldungen wie „Die digitale Signatur des Objekts konnte nicht bestätigt werden“, „Ein Zertifikat wurde explizit durch den Aussteller gesperrt“ oder „Eine Zertifikatkette zu einer vertrauenswürdigen Stammzertifizierungsstelle konnte nicht aufgebaut werden“. Die Datei ist damit ebenfalls erst mal nicht vertrauenswürdig.

Die nächste Zeile nennt ein Datum, und zwar entweder das der Erstellung des Zertifikats („Signing date“) oder das der Datei („Link date“), falls das Zertifikat fehlt. Es folgen derjenige, der das Programm veröffentlicht hat („Publisher“), die Firma, die das Programm geschrieben hat („Company“), Beschreibung („Description“), Produktname und -versionsnummer sowie die Versionsnummer der Datei. Bei „MachineType“ steht, ob das Programm 32- oder 64-bittig ist.

Die Ausgabe geht weiter mit sechs verschiedenen Hash-Werten. Es folgt die „VT detection“, die Zeile nennt das Ergebnis der Virustotal-Überprüfung. Im Idealfall steht hier „0/61“, wobei die Zahl hinter dem Schrägstrich mitunter leicht variiert – manches wird nicht von jedem



Wenn auch nur ein Virenscanner Alarm schlägt, öffnet sich eine Website mit detaillierten Angaben.

Scanner geprüft. Entscheidend ist die 0 vorne, denn dann hatte kein einziger Scanner etwas zu meckern. Der in der Zeile darunter stehende Link führt zur Ergebnis-Seite der Prüfung, dort können Sie sie detailliert betrachten.

Auswerten

Grundsätzlich sollten Sie alle Programme, die keine gültige Signatur aufweisen, erst einmal mit Vorsicht behandeln und auf weitere Details achten. Wenn einzelne Zeilen der Ausgabe nicht ausgefüllt sind (es steht dann dort „n/a"), deutet das auf Pfusch beim Erstellen der Datei hin. Das kann ein Alarmsignal sein, vor allem, wenn ein großes Unternehmen als Publisher genannt ist. Auch Ihnen oder gar Google unbekannte Publisher können ein Alarmsignal sein, müssen es aber nicht. Denn vielleicht ist es auch nur das Erstlingswerk eines bislang unbekannten, aber seriösen Programmierers.

Falls mindestens einer der Virustotal-Virenscanner Alarm schlägt, öffnet sich im Browser die Website von Virustotal mit einem detaillierten Bericht. Mitunter zeigen Symbole, wie andere Nutzer das Ergebnis einschätzen. Einen weiteren Anhaltspunkt gibt, ob die Alarme nur von Scanner-Exoten oder auch von den großen Scanner-Herstellern stammen. Alarme von Exoten kann man eher ignorieren. Mitunter handelt es sich allerdings doch nicht um einen Fehlalarm: Es kommt durchaus vor, dass ein Virenscanner einen besonders frischen Schädling vor allen anderen entdeckt, und das gilt für bekannte ebenso wie für exotische Scanner. Wer ganz sichergehen will, löscht die heruntergeladene Datei, statt sie zu starten.

Falls Virustotal.com den von Sigcheck übermittelten Hash nicht kennt, kann das ebenfalls ein Alarmsignal sein, muss aber nicht. Wenn Sie beispielsweise erstmals ein selbstgeschriebenes Skript untersuchen lassen, kann Virustotal die Datei zuvor ja noch nicht geprüft haben. Anders sieht es aus, wenn Virustotal den Hash einer prominenten Software nicht kennt. Das kann bedeuten, dass bloß soeben eine ganz neue Version erschienen ist (dann wiederholen Sie das Ganze noch mal nach einigen Stunden oder Tagen), aber auch, dass die Download-Seite infiltriert wurde. Denn normalerweise werden verbreitete Dateien so oft bei Virustotal hochgeladen, dass sie regelmäßig geprüft werden und der Hash demzufolge längst bekannt ist.

Empfehlung

Wenn die Prüfergebnisse eindeutig sind, ist die Empfehlung einfach: Sofern die Datei von einem bekannten Anbieter signiert ist und kein Virenscanner etwas zu meckern hat, ist sie wahrscheinlich harmlos – obwohl, um das noch einmal zu betonen, es keine Garantie dafür gibt, dass dem wirklich so ist. Wenn hingegen die Signatur fehlt oder Seltsamkeiten aufweist und gleich mehrere Virenscanner anschlagen, können Sie es mit den Hinweisen aus dem Kasten probieren – oder Sie gehen auf Nummer sicher und löschen die Datei kurzerhand. *(axv@ct.de)* **ct**

Literatur

[1] Olivia von Westernhagen, Werbung statt Spielspaß, Analysiert: PS3-Emulator als Schafspelz, c't 2/17, S. 172

[2] Olivia von Westernhagen, Feind aus dem Word-Dokument, Analysiert: Das Comeback der Makro-Malware, c't 5/17, S. 142

sigcheck.bat und sigcheck.exe:
ct.de/y8bm

Grenzfälle

Von Peter Siering

Für erfahrene Anwender kann es gute Gründe geben, die Einschätzung zu ignorieren, dass eine Software als gefährlich einzustufen ist – das muss allerdings im Einzelfall geprüft und abgewogen werden. Hilfreich dabei sind Einsichten in die Art und Weise, wie Antivirus-Software vorgeht: Sie prüft auf Signaturen, die eindeutig einen Schädling identifizieren. Sie sucht Muster, die erfahrungsgemäß typisch für Schädlinge sind (Heuristik). Sie fragt bei den Cloud-Diensten der Hersteller nach, ob dort eventuell bereits Erkenntnisse vorliegen, oder sendet Code-Proben unbekannter Programme dorthin, um sie dort eingehend zu untersuchen.

Obendrein stufen die Hersteller manche Software als „potentially unwanted application" (pua) ein: Programme, die sich als zweifelhafte Toolbar in Browsern breitmachen, die Windows-Passwörter zurücksetzen, die anderen Systemen übers Netz auf den Zahn fühlen, mit denen sich PCs fernsteuern lassen oder die Fenster verstecken. Wer so etwas auf einem PC der Schwiegermutter vorfindet, ohne dass die Herkunft klar ist, muss davon ausgehen, dass etwas faul ist. In einem Notfall-System wie unserem Notfall-Windows aus c't 26/16 machen solche Programme hingegen die Essenz aus.

Wenn man eine Datei von Virustotal analysieren lässt und nur eine Minderheit der dort eingespannten Programme Alarm schlägt, lohnt ein näherer Blick auf die Ergebnisspalte: Tauchen dort „gen" oder „heur" auf, dann handelt es sich eben um keinen eindeutigen Schädlingsfund, sondern nur um einen Verdacht – besonders der weniger prominente Teil der Zunft wittert schnell mal Gefahr, wo keine besteht. Stammt die Datei aus seriöser Quelle, die womöglich sogar diesen Umstand dokumentiert, muss man nicht gleich in Panik verfallen.

Eine nähere Untersuchung fällt schwer. Es gibt Dienste, an die man solche Dateien schicken kann und die sich in einer Sandbox an einer Analyse versuchen. Hundertprozentige Gewissheit liefert das nicht: Ein enthaltener Schädling könnte die Sandbox erkennen und verdächtige Funktionen erst gar nicht auslösen, etwa Netzwerkzugriffe, die ihn verrieten. Letztlich gibt es ohne detaillierte Code-Analyse keine abschließende Gewissheit – auch Software ohne Befund, obendrein aus vertrauenswürdigen Quellen, kann Überraschungen bergen.